AMENDMENTS TO THE CLAIMS

Upon entry of this amendment, the following listing of claims will replace all prior versions and listings of claims in the pending application.

IN THE CLAIMS

Please amend claims 1-4, 6-12, 14, 17 and 19-36 as follows:

1. (Currently Amended) A computer-implemented method for adaptively filtering URL messages routed across a network by generating exception rules to rejection rules based on attributes of URLs within messages previously received and rejected, the method comprising:

receiving, by a gateway, a first message specifying a first URL component;

rejecting, by the gateway, the first message based on a rejection rule, the rejection rule rejecting messages comprising the first URL component;

maintaining, by the gateway, a frequency for the first URL component, wherein the frequency is a function of a number of occurrences with which messages containing the first URL component were rejected and a number of occurrences with which messages containing descendants of the first URL component were rejected;

generating, by the gateway, an exception rule to the rejection rule for the first URL component and its descendants responsive to the frequency of the first URL component satisfying a set of constraints, the exception rule allowing to pass a message comprising the first URL component that is rejected by the rejection rule;

receiving, by the gateway, a second message specifying the first URL component, the second message rejected by the rejection rule; and

allowing, by the gateway, the second message to pass responsive to the exception rule.

2. (Currently Amended) The method of claim 1, wherein the set of constraints ~~a frequency~~ comprises the number of occurrences of the first URL component exceeding a threshold ~~and~~, the first URL component having no ~~children~~ descendents with a ~~frequency~~ number of occurrences above the threshold.

3. (Currently Amended) The method of claim 1, wherein the set of constraints requires ~~a~~ the frequency exceeding a threshold.

4. (Currently Amended) The method of claim 1, further comprising applying the exception rule to determine whether to allow URLs comprising the ~~selected~~ first URL component and its descendants to pass.

5. (Original) The method of claim 2, wherein the threshold is a product of a total number of URL messages over a time interval and a percentage of the messages that should be allowed.

6. (Currently Amended) The method of claim 1, wherein the exception rule is generated by inferencing a scalar data type of the descendants of the ~~selected~~ first URL component.

7. (Currently Amended) The method of claim 1, wherein the frequency is a direct count of the occurrences of the first URL component.

8. (Currently Amended) The method of claim 1, wherein the frequency is a weighted count of the occurrences of the first URL component.

9. (Currently Amended) A computer-implemented method for adaptively filtering URL messages routed across a network by generating exception rules to rejection rules based on attributes of URLs within messages previously received and rejected, the method comprising:

receiving, by a gateway a plurality of messages, each message specifying a first URL component;

rejecting, by the gateway the plurality of messages based on a rejection rule, the rejection rule rejecting messages comprising a URL component;

storing, by the gateway rejected URLs in a trie structure, wherein each node in the trie structure is associated with ~~a~~ the URL component;

maintaining, by the gateway a frequency for each node associated with a URL component, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node were rejected and a number of occurrences with which descendants of the URL component were rejected;

generating , by the gateway an exception rule to the rejection rule for a node associated with the first URL component and its descendants responsive to the frequency of the first URL component satisfying a set of constraints, the exception rule allowing to pass a message comprising the URL component that is rejected by the rejection rule;

receiving, by the gateway ~~a~~ the message specifying the first URL component, the message rejected by the rejection rule; and

allowing the message to pass responsive to the exception rule.

10. (Currently Amended) The method of claim 9, further comprising applying the exception rule to determine whether to allow URLs associated with the ~~selected~~ node and its descendants to pass.

11. (Currently Amended) The method of claim 9, wherein the set of constraints requires a ~~number of occurrences~~ frequency associated with the node exceeding a threshold.

12. (Currently Amended) The method of claim 9, wherein the set of constraints requires a number of occurrences associated with the node exceeding a threshold, the node ~~and~~ having no ~~children~~ descendants with a number of occurrences above the threshold.

13. (Original) The method of claim 11, wherein the threshold is a product of a total number of URL messages over a time interval and a percentage of the messages that should be allowed to pass.

14. (Currently Amended) The method of claim 9, wherein the exception rule is generated by inferencing a scalar data type of the descendants of the ~~selected~~ first URL component.

15. (Original) The method of claim 9, wherein the frequency is a direct count of a number of occurrences of the URL component.

16. (Original) The method of claim 9, wherein the frequency is a weighted count of a number of occurrences of the URL component.

17. (Currently Amended) A system for adaptively filtering URL messages routed across a network, by generating exception rules to rejection rules based on attributes of URLs within messages previously received and rejected, the system comprising:

a learning engine ~~adapted to perform the steps of~~ of a device:

storing rejected URLs in a trie structure, wherein each node in the trie structure is associated with a URL component, and wherein the rejected URLs are rejected based on a rejection rule, the rejection rule rejecting URLs comprising a URL component;

maintaining a frequency for each node associated with ~~a~~ the URL component, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node were rejected and a number of occurrences with which descendants of the URL component were rejected, and

generating an exception rule to the rejection rule for a first node and its descendants, responsive to the frequency of the URL component associated with the first node satisfying a set of constraints, the exception rule allowing to pass URLs comprising the URL component that are rejected by the rejection rule; and

a filter of the device ~~configured to~~ applying the exception rule to a rejected URL to determine whether to allow the first node and its descendants.

18. (Canceled)

19. (Currently Amended) The system of claim 17, wherein the set of constraints requires a number of occurrences associated with the first node exceeding a threshold ~~and~~, the first node having no ~~children~~ descendants with a number of occurrences above the threshold.

20. (Currently Amended) The system of claim 17, wherein the set of constraints requires ~~a~~ the frequency associated with the first node exceeding a threshold.

21. (Currently Amended) The system of claim ~~19~~ 20, wherein the threshold is a product of a total number of URL messages over a time interval and a percentage of the messages that should be allowed.

22. (Currently Amended) The system of claim 17, wherein the exception rule is generated by inferencing a scalar data type of the descendants of the ~~selected node~~ URL component associated with the first node.

23. (Currently Amended) The system of claim 17, wherein the frequency for each node is a direct count of the number of occurrences of the URL component associated with the corresponding node.

24. (Currently Amended) The system of claim 17, wherein the frequency for each node is a weighted count of the number of occurrences of the URL component associated with the corresponding node.

25. (Currently Amended) A computer program product comprising: a computer-readable medium having computer program code embodied therein for adaptively filtering URL messages routed across a network by generating exception rules to rejection rules based on attributes of URLs within messages previously received and rejected, the computer program code adapted to:

store rejected URLs in a trie structure, wherein each node in the trie structure is associated with a URL component and each node associated with a URL component maintains a frequency, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node were rejected, and wherein the rejected URLs are rejected based on a rejection rule, the rejection rule rejecting URLs comprising a first URL component; and

generate an exception rule to the rejection rule for a first node and its descendants responsive to the frequency of the a URL component associated with the first node satisfying a set of constraints, the exception rule allowing to pass URLs comprising the first URL component that are rejected by the rejection rule.

26. (Currently Amended) The computer program product of claim 25, wherein each node associated with a URL component maintains a frequency, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node was rejected and a number of occurrences with which descendants of the ~~URL component~~ node were rejected.

27. (Currently Amended) The computer program product of claim ~~26~~ 25, wherein the set of constraints requires a ~~frequency~~ number of occurrences associated with the first node exceeding

a threshold, the first node ~~and~~ having no ~~children~~ descendants with a ~~frequency~~ number of occurrences above the threshold.

28. (Currently Amended) The computer program product of claim ~~26~~ 25, wherein the set of constraints requires the ~~a~~ frequency associated with the first node exceeding a threshold.

29. (Currently Amended) The computer program product of claim 25, wherein the computer program code is further adapted to apply the exception rule to determine whether to allow ~~the selected~~ URLs associated with the first node and its descendants to pass.

30. (Currently Amended) The computer program product of claim ~~27~~ 28, wherein the threshold is a product of a total number of URL messages over a time interval and a percentage of the messages that should be allowed to pass.

31. (Currently Amended) The computer program product of claim 25, wherein the exception rule is generated by inferencing a scalar data type of the descendants of the ~~selected~~ URL component associated with the first node.

32. (Currently Amended) A computer-implemented method for adaptively filtering URL messages routed across a network, by generating exception rules to rejection rules based on attributes of URLs within messages previously received and rejected, the method comprising:

storing rejected URLs in a trie structure, wherein the rejected URLs are rejected based on a rejection rule, the rejection rule rejecting URLs comprising a first URL component, and

wherein each node in the trie structure is associated with a URL component; and each node associated with a URL component maintains a frequency, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node was rejected; and

and generating an exception rule to the rejection rule for a first node and its descendants, responsive to the frequency of the URL component associated with the first node satisfying a set of constraints, the exception rule allowing to pass URLs comprising the first URL component that are rejected by the rejection rule.

33. (Currently Amended) The method of claim 32, further comprising maintaining a frequency for each node associated with a URL component, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node was rejected and a number of occurrences with which descendants of the ~~URL component~~ selected node were rejected.

34. (Currently Amended) The method of claim 32, further comprising applying the exception rule to determine whether to allow the ~~selected~~ URLs associated with the first node and its descendants to pass.

35. (Currently Amended) The method of claim 32, wherein the set of constraints requires ~~a number of occurrences~~ the frequency associated with the first node exceeding a threshold.

36. (Currently Amended) The method of claim 32, wherein the set of constraints requires a number of occurrences associated with the first node exceeding a threshold ~~and~~, the first node having no ~~children~~ descendants with a number of occurrences above the threshold.

37. (Original) The method of claim 35, wherein the threshold is a product of a total number of URL messages over a time interval and a percentage of the messages that should be allowed.

38. (Currently Amended) The method of claim 32, wherein the exception rule is generated by inferencing a scalar data type of the descendants of the ~~selected~~ URL component associated with the first node.

39. (Original) The method of claim 33, wherein the frequency is a direct count of the number of occurrences of the URL component associated with the selected node.

40. (Original) The method of claim 33, wherein the frequency is a weighted count of the number of occurrences of the URL component associated with the selected node.